

HMDC Presents... SPECPOL: Review Quiz

HMDC Presents... Review Quiz: SPECPOL: Corporate Surveillance, Accountability and Privacy

We take this quiz after we have read the full SPECPOL research report. When we finish, we check our answers in the Answer Key at the end. For every question we missed, we go back to the report section named in the key and reread it, so that the idea is clear before committee.

PART 1 THE TOPIC

These questions cover the harms, the major solutions, and the advantages and disadvantages of each solution.

1. Our report says the spyware problem is an industry, not a single harmful company. Which fact from the UN Human Rights Office best supports this?

- A. NSO Group admitted its customers target 12,000 to 13,000 people each year.
- B. More than 500 companies reportedly develop and sell surveillance tools to governments, and at least 65 governments had acquired commercial spyware.
- C. Pegasus was used against at least 189 journalists.
- D. Apple fixed the flaw that Paragon's Graphite spyware used against journalists.

2. Google's Threat Analysis Group found that commercial surveillance vendors are behind roughly half of the known zero-day exploits aimed at Google products and Android devices. Why does this matter for every phone user, not only for spyware targets?

- A. Zero-day exploits only work on phones owned by journalists.
- B. Google has stopped all zero-day attacks since 2024.
- C. By keeping secret software flaws unfixed, spyware firms make everyone's phone less safe, which gives delegates a security argument as well as a human rights argument.
- D. Zero-day exploits are legal everywhere, so they cannot be regulated.

3. Researchers at Duke University bought sensitive data about United States military members from data brokers for as little as 12 cents per record. What does the report say this shows?

- A. The data economy is a security problem, because almost anyone, including a foreign government, may be able to buy sensitive data.
- B. Data brokers always check carefully who their buyers are.
- C. Only soldiers are harmed by data brokers.
- D. Selling personal data is already tightly controlled by law in the United States.

4. Solution 1 is a global moratorium (a temporary stop) on spyware sales. According to the Carnegie Endowment, what is a major disadvantage of this solution?

- A. UN human rights experts have never supported a moratorium.
- B. A moratorium would immediately become a binding treaty.
- C. A moratorium would only apply to autocracies.
- D. When some vendors are stopped, buyers move to newer suppliers, so a pause that only some countries respect may just shift business elsewhere.

5. Solution 2 asks for stronger export controls. Why does the report say the Wassenaar Arrangement has not meaningfully limited the spread of surveillance tools?

- A. It has only three member states.
- B. It is non-binding, it was built to reduce military threats, and it lacks guidelines and enforcement on human rights.
- C. It was created by the UN General Assembly in 2024 and has not started work yet.
- D. It bans all exports of software, so companies ignore it.

6. In a six-month trial, British Transport Police used live facial recognition in London railway stations. What was the result?

- A. It scanned more than half a million faces, produced only one alert, which was an incorrect identification, and led to no arrests.
- B. It led to hundreds of arrests and was ended because it worked so well.
- C. It was banned by the European Union's AI Act before it started.
- D. It scanned only people who agreed to be scanned.

PART 2 THE UNITED NATIONS

These questions cover the main UN resolutions and UN bodies: their names, their years, and what they did.

1. Which resolution started the UN's modern work on digital privacy, and how was it adopted?

- A. A/RES/79/243, adopted in 2024 by a close vote.
- B. A/HRC/RES/26/9, adopted in 2014 by a vote of 20 to 14.
- C. A/RES/68/167, "The right to privacy in the digital age," adopted by the General Assembly in 2013 without a vote.
- D. A/RES/217 A (III), adopted in 1966 by the Human Rights Council.

2. In 2011 the Human Rights Council endorsed the UN Guiding Principles on Business and Human Rights (resolution A/HRC/RES/17/4). What is the main limit of these principles?

- A. They are voluntary for companies, so they create no binding duties.
- B. They apply only to European companies.
- C. They were replaced by a binding treaty in 2014.
- D. They cover governments only and say nothing about companies.

3. What can the UN Special Rapporteur on the right to privacy do?

- A. Fine companies that break privacy rules.
- B. Investigate and recommend, but not enforce.
- C. Arrest people who use spyware.
- D. Approve or block every surveillance technology sale in the world.

4. In 2014 the Human Rights Council voted to create a working group to write a binding treaty on business and human rights (A/HRC/RES/26/9). What does the vote of 20 in favour, 14 against and 13 abstentions show?

- A. Every state agreed that companies need binding rules.
- B. The treaty was finished and signed that same year.
- C. Only developing countries voted against it.
- D. There is a real political divide, because several states whose companies dominate tech, including the United States, the United Kingdom, Germany, France and Japan, voted against it.

5. The UN Convention against Cybercrime (A/RES/79/243, 2024) includes human rights safeguards in Articles 6 and 24. Why does the report say these safeguards may be weak?

- A. The Convention bans all surveillance, so no safeguards are needed.
- B. The safeguards rely on each country's own domestic laws, so where those laws are weak, the protection is weak too.
- C. The Convention entered into force in 2013, before smartphones were common.
- D. The safeguards apply only to companies, not to governments.

PART 3 INTERNATIONAL EFFORTS

These questions cover efforts outside or beside the United Nations, and the gaps those efforts leave open.

1. What is Convention 108 of the Council of Europe, and where does its modernised version, Convention 108+, stand?

- A. It is a voluntary code for spyware buyers, and it has been signed by 27 states.
- B. It is a UN resolution from 2013, and it is already fully in force worldwide.
- C. It was the first legally binding international treaty on data protection (1981), and Convention 108+ had 34 of the 38 ratifications it needs as of May 2026.
- D. It is an AI treaty that covers national security activities.

2. The Pall Mall Process, launched by the United Kingdom and France in 2024, produced a Code of Practice for States in 2025. What gap does the report point out?

- A. The Code is non-binding, and many major spyware buyers are absent from it.
- B. The Code has no pillars or principles.
- C. The Code is binding on every UN member state.
- D. The Code applies only to private citizens.

3. The Council of Europe's Framework Convention on Artificial Intelligence covers private companies and lists privacy as a basic principle. What weakness does the report highlight?

- A. Only European states may sign it.
- B. Activities related to national security do not have to follow its provisions, which leaves out the area where spyware is most used.
- C. It does not mention privacy or data protection at all.
- D. It was rejected by the European Union.

4. In October 2025 a United States judge ordered NSO Group to stop targeting WhatsApp users. Why does the report treat this case as important?

- A. It was the first time a UN body punished a spyware company.
 - B. It shut down NSO Group completely.
 - C. It forced every government to stop buying Pegasus.
 - D. A private company used a national court to hold a spyware maker responsible, something no UN body has done.
-

THINK LIKE A DELEGATE

These questions have no single correct answer. We write a short paragraph for each, then compare our answer with the points a strong answer includes in the Answer Key.

- 1.** Our country buys surveillance tools for police work, but we also want to stop spyware from being used against journalists. What should we argue for in committee, and why?
 - 2.** Our country is one of the roughly 57 countries without a data protection law. What should we ask SPECPOL to do for countries like ours, and why?
 - 3.** A company sells spyware to a government, and that government uses it against a journalist in another country. Who should be held responsible, and why?
-

ANSWER KEY

We check each answer, read the reason, and reread the named section for any question we missed.

PART 1 THE TOPIC

1. **B.** The report counts more than 500 companies and at least 65 government buyers, which shows a whole market rather than one firm (Part 1, Section 1A, entry 2).
2. **C.** Spyware firms hoard secret software flaws, which leaves everyone's devices less safe and turns the issue into a security question (Part 1, Section 1A, entry 6).
3. **A.** The researchers found brokers checked buyers inconsistently, so foreign or criminal actors could buy sensitive data to profile or blackmail people (Part 1, Section 1A, entry 12).
4. **D.** Carnegie found that when vendors such as FinFisher and Hacking Team faded, buyers simply moved to newer suppliers (Part 1, Section 1B, Solution 1, entry 22).
5. **B.** The UN Special Rapporteur explains that Wassenaar is non-binding, was built for military threats and lacks human rights enforcement (Part 1, Section 1B, Solution 2, entry 24).
6. **A.** The trial scanned over half a million faces at high cost and produced one incorrect alert and no arrests (Part 1, Section 1B, Solution 5, entry 31).

PART 2 THE UNITED NATIONS

1. **C.** The General Assembly adopted A/RES/68/167 without a vote on December 18, 2013, and has updated it every two years since (Part 2, Table of Resolutions and entry 35).
2. **A.** The Guiding Principles set out "Protect, Respect and Remedy," but they remain voluntary for companies (Part 2, entry 36 and Section 2C).
3. **B.** The Special Rapporteur, created in 2015 by resolution 28/16, can investigate and recommend but cannot enforce (Part 2, entry 38).
4. **D.** The split vote, with major tech home countries voting against, shows a lasting divide over binding rules for companies (Part 1, Section 1B, Solution 3, entry 25, and Part 2, Table of Resolutions).
5. **B.** Articles 6 and 24 depend on domestic law, so protection is only as strong as each country's own laws (Part 2, entry 41).

PART 3 INTERNATIONAL EFFORTS

1. **C.** Convention 108 opened in 1981 as the first binding data protection treaty, and Moldova became the 34th ratifier of Convention 108+ in May 2026, with 38 needed (Part 3, entries 46 and 47).
2. **A.** The Code is voluntary and supported by a small, mostly Western group of states (Part 3, entries 51 and 52).
3. **B.** The treaty exempts national security activities, exactly where spyware is most used (Part 3, entry 48).
4. **D.** WhatsApp, a private company, won a court order against NSO Group in a United States court, a path no UN body has offered victims (Part 3, entry 57).

THINK LIKE A DELEGATE

1. **Buying tools and protecting journalists.** A strong answer accepts that both democracies and autocracies buy spyware, so a full ban may not pass, and argues instead for strict conditions on use. It borrows the European Parliament's list (a judge's approval, a set purpose, a short time limit, notifying targets afterwards, an independent lab), mentions buyer rules such as the 2023 United States order and the Pall Mall Code of Practice, and explains that these conditions reduce harm without ending lawful police work (Part 1, Section 1A, entry 3; Part 3, entries 52, 62 and 63).
2. **Helping countries without data laws.** A strong answer asks for capacity-building, meaning money and experts to write and enforce data protection laws, and points out that heads of state already promised this in the Global Digital Compact. It may suggest joining Convention 108+, which is open to countries outside Europe, and may raise data sovereignty, while noting the disadvantage that developing countries lack enforcement resources and should not be forced to copy European rules (Part 1, Section 1B, Solution 4, entry 27; Part 2, entry 40; Part 3, entries 46 and 64; Discussion Question 5).
3. **Deciding who is responsible.** A strong answer uses the Guiding Principles: the state must protect, the company must respect human rights, and the victim must have access to remedy. It explains that firms can rename themselves or move countries, so rules may need to follow investors and founders as well, and it may support the binding business and human rights treaty or a remedy fund for victims, while admitting that treaty talks have been slow since 2014 (Part 1, Section 1A, entries 4 and 5; Part 1, Section 1B, Solution 3; Part 1, Section 1C; Part 2, entry 36).